PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

Appl. No. 10/631,899
Doc. Ref. AA8

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPE ... (PCT)

(51) International Patent Classification 6 :
G07C 9/00, G06F 1/00

A1

(11) International Publication Number: WO 98/12670

(43) International Publication Date: 26 March 1998 (26.03.98)

(21) International Application Number: PCT/CA97/00663

(22) International Filing Date: 15 September 1997 (15.09.97)

(30) Priority Data:
08/715,432 18 September 1996 (18.09.96) US

(71) Applicant *(for all designated States except US)*: DEW ENGINEERING AND DEVELOPMENT LIMITED [CA/CA]; 3429 Hawthorne Road, Ottawa, Ontario K1G 4G2 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BORZA, Stephen, J. [CA/CA]; 495 Metcalfe Street, Ottawa, Ontario K1S 3N3 (CA). FREEDMAN, Gordon [CA/CA]; 41 Elvaston Avenue, Nepean, Ontario K2G 3Y1 (CA).

(74) Agent: FREEDMAN, Gordon; Neil Teitelbaum & Associates, 834 Colonel By Drive, Ottawa, Ontario K1S 5C4 (CA).

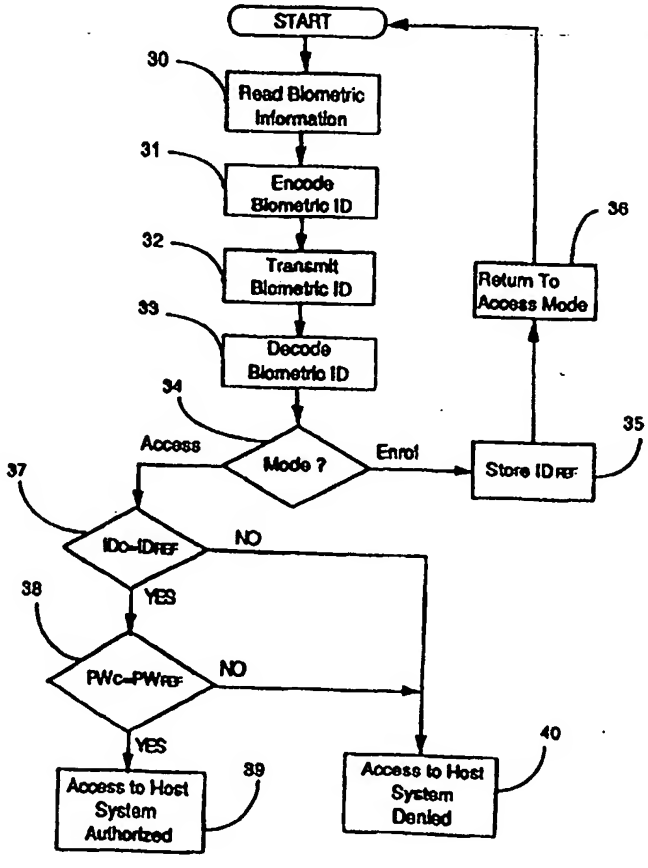
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(54) Title: BIOMETRIC IDENTIFICATION SYSTEM FOR PROVIDING SECURE ACCESS

(57) Abstract

A portable device is disclosed for receiving biometric information and for providing a signal in dependence thereon to a remote receiver. The device comprises a biometric sensor for imaging fingerprints, a processor for encoding the input biometric information, an infrared transmitter for transmitting the encoded biometric information to a receiver, and a power source. The device can be implemented in a watch, key chain, ID badge or a credit card.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

BIOMETRIC IDENTIFICATION SYSTEM FOR PROVIDING SECURE ACCESS

Field of the Invention

This invention relates generally to personal identification systems and more particularly relates to a biometric security identification system (BSIS).

Background of the Invention

Biometric security identification systems, such as fingerprint scanning and input devices are becoming more commonplace as the need to validate authorized users of computers, databases, and secure spaces grows. As computers become more miniaturized, so too are other communication and security devices decreasing in size. One of the more important reasons, however, to miniaturize electronic devices is to lessen the burden of porting them.

The use of security systems is generally well known. Their use is increasing with greater availability of digital electronic components at a relatively low cost. Such systems are known for securing buildings, banks, automobiles, computers and many other devices. For example, U.S. Pat. No. 4, 951, 249 discloses a computer security system which protects computer software from unauthorized access by requiring the user to supply a name and a password during the operating system loading procedure ("boot-up") of a personal computer (PC). This is accomplished by the insertion of a special card into an input/output expansion slot of the PC. During the loading of the operating system of the PC, the basic input/output system (BIOS) scans memory addresses of the card for an identification code, consisting of a 55AA hex code. When this hex code is located, the BIOS instructions are vectored to the address where the target hex code resides and instructions at the following addresses are executed as part of the initialization routines of the system boot-up procedure.

This PC security system, utilizing password protection, is typical of many systems that are currently available. Password protection requires a user's name and a password associated with that user's name. Only once an associated password is detected for a valid user's name does the PC complete the boot-up routine. Though passwords may be useful in some instances, they are inadequate in many respects. For example, an unauthorized skilled

user with a correct password in hand, can gain entry to such a processor based system. Yet another undesirable feature of the foregoing system is that passwords on occasion are forgotten; and furthermore, and more importantly, passwords have been known to be decrypted.

As of late one of the most ubiquitous electronic components is the digital processor. Multi-purpose and dedicated processors of various types control devices ranging from bank machines, to cash registers and automobiles. With ever increasing use of these processor based devices, there is greater concern that unauthorized use will become more prevalent. Thus, the verification and/or authentication of authorized users of processor based systems is a burgeoning industry.

Alarms and security systems to warn of unauthorized use of automobiles and other processor controlled systems are available, however, these security systems have been known to be circumvented. Unfortunately, many commercially available solutions aimed at preventing theft or unauthorized use of automobiles have also been circumvented. As of late, initiatives have been underway in the security industry, to provide biometric input devices to validate users of electronic and other systems, that are to have restricted access. One limitation associated with many typical commercially available biometric systems is the large physical size of the imaging devices. Concern with placing a biometric input device in an location that is accessible to the public is the risk of the input device being vandalized.

In the field of digital and analog communications, wireless devices are becoming more commonplace. Inexpensive computer systems are currently commercially available wherein printers communicate with computers which in turn communicate with other computers via infra red transmitters and receivers. Other devices, using other optical communication systems, such as data transmitting/receiving wrist watches are now available in department stores at substantially affordable prices; these wrist watches include processors and software for communication with a computer and for downloading and uploading small amounts of data as required.

Object of the Invention

It is an object of this invention to provide a portable biometric input device for sensing input biometric data, and transmitting the data to a receiver.

Summary of the Invention

In a first broad embodiment the invention seeks to provide a portable biometric input device comprising: biometric sensing means for sensing biometric input information. generating biometric data therefrom, and providing the biometric data in relation to the sensed biometric input information; transmission means for receiving at least an aspect of the biometric data and for transmitting a signal in dependence upon the at least an aspect of the biometric data; and a battery for providing power to the device.

In an embodiment, the transmission means is a wireless transmission means for transmitting a signal in dependence upon the at least an aspect of the biometric data.

In an embodiment. the transmission means comprises a biometric data encoder and an infrared transmitter for transmitting a signal in dependence upon the at least an aspect of the biometric data.

In an embodiment. the device further comprises storage means for storing data related to said biometric data.

In an embodiment, the device further comprises processor means for processing the biometric data.

In an embodiment, the processor means is for comparing the biometric data with previously stored biometric data to provide comparison results; and the signal in dependence upon at least an aspect of the biometric data comprises a signal in dependence upon the comparison results.

In an embodiment, the device further comprises means to receive a password and wherein the transmission means is for transmitting a signal in dependence upon at least an aspect of the biometric data and the password.

In an embodiment, the device further comprises means to receive a password and wherein the processor means is for comparing the biometric data with previously stored biometric data and the password and a previously stored password to provide comparison results; and the signal in dependence upon at least an aspect of the biometric data comprises a signal in dependence upon the comparison results.

In an embodiment, the device further comprises means for encrypting at least an aspect the biometric data; and the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data.

In an embodiment, the means for encrypting the biometric data comprise public/private key encryption means.

Alternatively, the means for encrypting the biometric data comprise session key encryption means.

In an embodiment, the biometric input means is a fingerprint imaging device.

In an embodiment, the device further comprises a housing in the form of a watch casement and a watch face.

In an embodiment, the biometric input means comprises associated electronic circuitry and conductive pads disposed on the watch face.

In a further broad embodiment, the invention seeks to provide a portable biometric input sensor comprising: an array of sense elements spaced apart and comprising a sensing electrode for sensing biometric input; drive means coupled to at least some of the sense

elements for controlling and addressing each of the at least some sense elements according to a predetermined sequence, for receiving a signal in dependence upon the biometric input, and for providing biometric data in dependence upon the sensed biometric input; processor means for processing biometric data; and, wireless transmission means for transmitting to a receiver a signal that corresponds to at least an aspect of the biometric data.

In an embodiment, the device further comprises means for encrypting the biometric data further comprising means for encrypting at least an aspect the biometric data; and the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data.

In an embodiment, the means for encrypting the biometric data comprise public/private key encryption means.

In an embodiment, the means for encrypting the biometric data comprise session key encryption means.

In another broad embodiment the invention seeks to provide a biometric security identification system comprising: a portable transmitting module comprising a biometric sensing means, means for encoding biometric data and wireless transmission means for transmitting the encoded biometric data as an encoded signal; and a receiving module comprising means for receiving the encoded signal, means for extracting the encoded biometric data, and means for comparing the encoded biometric data with predetermined reference values, and means for authorizing access to a host system.

In an embodiment, the biometric sensing means comprises a fingerprint scanner.

In an embodiment, the device further comprises means for encrypting the biometric data further comprising means for encrypting at least an aspect the biometric data; the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data; and the means for extracting the

encoded biometric data comprises means for decrypting and for extracting the encoded biometric data.

In an embodiment, the means for encrypting the biometric data comprise public/private key encryption means.

In an embodiment, the means for encrypting the biometric data comprise session key encryption means.

In yet another broad aspect, the invention seeks to provide a portable biometric input device comprising: sensing means including a platen upon which to rest a finger, said sensing means for sensing the presence and location of fingerprint ridges upon the device; processor means for processing sensed data; and, wireless transmission means for transmitting a signal that corresponds to at least an aspect of the sensed data; and a battery for providing power to the device.

The advantages of a system in accordance with this invention are numerous. For example, providing a lightweight fingerprint input transducer capable of wireless communications with a remote system obviates the requirement of securing the input transducer from vandals and prevents tampering therewith. Providing an input sensor that serves as a user's personalized key, offers distinct and obvious advantages. Firstly, the sensor may be protected by the user, being his or her own personal device, and furthermore, a user's personalized sensor may communicate with several different devices that require validation in the form of a users biometric input data; for example, the input sensor may provide a valid access code in the form of a biometric key, to unlock a locked car door, a house door, and/or to provide access to a banking machine or a computer. Furthermore, a user's personal sensor can be programmed with its own identification key which can accompany a user's biometric data in the validation process, to validate both the sensor and the user.

Brief Description of the Drawings

Exemplary embodiments of the invention will now be discussed in conjunction with the attached drawings in which:

Fig. 1 is a block diagram of the biometric security identification system (BSIS) according to the invention;

Fig. 2 is a simplified diagram of a sensing device for use with the present invention showing an array of sensing elements together with associated addressing circuitry;

Fig. 3 is a simplified diagram of a sensing element for use with the present invention;

Fig. 4 is a schematic diagram of an amplifier circuit for use with the present invention;

Fig. 5a is a digital watch according to the present invention;

Fig. 5b is an analogue watch according to the invention;

Fig. 6 is a block diagram of the transmitting module of Fig. 1;

Fig. 7 shows a block diagram of the receiving module of Fig. 1;

Fig. 8 is a flowchart for illustrating a mode of operation of an embodiment of a BSIS according to the present invention;

Fig. 9 is a flowchart for illustrating a mode of operation of an embodiment of a BSIS according to the present invention;

Fig. 10 is a flowchart for illustrating a mode of operation of an embodiment of a BSIS according to the present invention further comprising bi-directional communication;

Fig. 11 is a flowchart for illustrating a mode of operation of an embodiment of a BSIS using bi-directional communication and a time out according to the present invention;

Fig. 12 is a biometric credit card according to the present invention;

Fig. 13 is a device according to the present invention incorporated into a keychain and using infrared wireless communication; and

Fig. 14 is a device according to the present invention incorporated into a keychain and using RF wireless communication.

Detailed Description

Fig. 1 illustrates the block diagram of a biometric security identification system (BSIS) according to the invention. The system comprises a transmitting module **10** and a receiving module **20** connected over a transmission channel in the form of a wireless transmission channel. The transmitting module **10** measures a biometric characteristic of a person requesting access to a protected host system and converts the biometric characteristic

into a biometric identification (ID) code. The transmitter module is adapted to be carried or worn by the user, and therefore can take any suitable form, such as a wrist watch, a badge, a wallet, etc.

The biometric information may be accompanied by a password for increased security of the identification process. In this way, access to the protected host system is denied to unauthorized users, who may have a similar biometric ID. Similar biometric ID may occur if the transducer has a low sensitivity, for example for cost or/and miniaturization reasons. The password could be any machine readable code like a PIN, an account number, or a time-varying code. Selected passwords can be unique to the watch itself, or they can be chosen by the user.

It is apparent that various types of transducers may be used, such as image or temperature transducers, electromagnetic field sensors, optical sensors, etc. Preferably, the sensitivity of the transducer allows for capture of biometric data which reasonably distinguishes the user. In an embodiment, the transmitting module is in the form of a wrist watch provided with a fingerprint reader and described in more detail below.

The biometric ID is transmitted to receiving module **20**, which is attached to a host system. The transmission is preferably made by modulating an infrared (IR) carrier with the biometric ID, but any other type of communication between the transmitting module **10** and receiving module **20** may be used. Preferably wireless communication means are used as dictated by selected design parameters, such as the distance between the modules, the power budget, etc. Preferably, and for obvious security reasons, a wireless communication means employed should minimize the risk of interception and recording of a biometric ID.

At receiving module **20**, the biometric ID is compared to a reference ID pre-stored in a memory. If the current biometric ID (IDC) matches a reference ID (IDREF), access to the host system is authorized. The host system could be a computer system, an ATM banking machine, a door latch or any other system which must be secured against unauthorized

access. In an alternative embodiment, the biometric ID is compared in the transmitting module **10** and an access code is sent to the receiving module **20** for comparison.

Referring to Fig. 2. part of a sensing device for use in an embodiment of the present invention and implemented on a semiconductor chip is shown comprising a single active matrix addressed sensing pad **119** having an X-Y array of sense elements consisting of r rows (1 to r) with c sensing elements **117** in each row. In practice there may be about 300 rows and 200 columns of regularly-spaced elements occupying an area of approximately 2 cm x 3 cm. This area is for accepting a fingertip for scanning. Should such a sensing pad **119** be made larger, it could be used for scanning other items such as a palm of a hand.

Sensor elements **117** are disposed in such a fashion that they are capable of distinguishing the smallest desired feature of a fingerprint. Preferably, the placement and spacing of the sensor elements allow an image of a fingerprint, once scanned, to contain all required features for analysis. The sensing element **117** is smaller than half the smallest sensible feature size allowing a suitable image to be generated. Empirical studies reveal that a square plate of about 50 μm edge length is suitable for fingerprint sensing. Although the apparatus is described with reference to an array of sensing elements **117** having substantially square shape, it is possible to use different configurations of sensing elements **117** such as concentric circles or a spiral and different shapes such as triangles, circles, or rectangles.

The array of sensing elements **117** is connected through an analog switch matrix to facilitate reading the fingerprint image out of the sensing array **119**. Timing and sequencing logic **116** selects each element in the array in turn to produce a complete image of a fingerprint presented to the device. The signal may be output directly as an analog signal or may be converted to a digital signal prior to output from the device.

The sensing pad **119** further comprises a ground ring **115** and bonding pads **118** designed for connection to other components or to packaging. The ground ring **115** also serves to provide a common ground for the sensing pad. Accordingly, it is important that the ground ring **115** and integrated circuit elements be designed so as to minimize noise to each

sensing element **117**. The signal to noise ratio that is acceptable will vary between applications and should be adjusted to meet the needs of a specific design. When possible, packaging should be selected to limit noise.

Referring to Fig. 3, a single sensing plate **120** is shown. Such a sensing plate **120** is designed to be used in arrays and preferably is smaller than half the smallest sensible feature size as indicated above. Charge sensing electrode **121** is connected to an active element which is shown as a three terminal switching device in the form of a field effect transistor (FET) having a source, a drain, and a gate **126**. The gate **126** is connected to the sensing electrode **121** by an interconnect **124**. Disposed between the gate **126** and the transistor **130** is a gate oxide **127**. Such transistor configuration is known in the art.

Above the charge sensing electrode **121** is disposed an overglass **122** which serves to protect the charge sensing electrode **121** and to space the electrode and a fingertip presented thereto. Below the charge sensing electrode **121** is disposed a field oxide **125**. A finger placed against the overglass **122** induces charge in the charge sensing electrode **121**. By amplifying the charges induced by a fingertip on the charge sensing electrode **121** with an amplifier circuit such as is shown in Fig. 4, the induced charges can be rendered easily distinguishable.

Referring to Fig. 4, a sensing pad **120** is electrically grounded. A second side is connected through electrostatic discharge protection **131** in the form of resistors and diodes. A filter circuit **132** and **133** improves circuit operation. Transistors **134, 135, 136**, and **137** provide amplification of induced voltages allowing a signal at an output of transistor **136** to be digitized by a low cost A/D converter.

Assuming that the charge density on the fingertip is substantially even, induced charges on the charge sensing electrode **121** will depend solely on the distance between the charge sensing electrode **121** and the skin of the fingertip inducing the charge. Further, as the induced charge falls off with the distance, the closest skin of the fingertip will induce a larger proportion of the charge. The sensor is employed in the above fashion to image fingertips.

Referring to Fig. 5a, a watch is shown comprising (in part) the present invention. The watch **50** is secured in place on a person's wrist for example by way of a strap **51**. Alternative methods such as a chain as is common in pocket watches, a pouch (not shown), velcro, a pin, or means for securing the watch to a sporting apparatus may also be used. A time display means **52** in the form of an LCD display, an LED display, an analogue time display, a voice generated time, or a Braille time display is disposed upon the watch **50** in a conventional manner. Preferably, the time display means **52** is offset to allow for sufficient contiguous surface area for a biometric sensor **53**. Alternatively, the biometric sensor **53** is designed to be superimposed upon the time display means **52** and not interfere therewith as shown in Fig. 5b. An emitter port in the form of an infra red emitter port **55** is located on the watch **50** such that light emitted from the infra red port **55** is directed toward a sensor (not shown) in use. In Fig. 5a and Fig. 5b, the infra red emitter port **55** is located on the top of the watch above the face and pointing substantially coplanar to the watch face. In this orientation, an emitted signal is directed away from the body of a user and forward during normal use.

The biometric sensor means **53** is of the form described above and shown in Figs. 2, 3, and 4. Alternatively, the biometric sensor means **53** is a capacitive fingerprint scanner requiring pre-charging as are well known in the art. Further alternatively, the biometric sensing means **53** is an optical biometric scanning device in the form of a retinal scanner, an optical fingerprint scanner, an optical palm scanner, or any other suitable (and portable) biometric sensing device.

Referring to Fig. 5b, an analogue watch **150** is shown. Analogue watches of this type are well known and are in common use. On to the face of the analogue watch **150** are deposited a plurality of metal pads 155 and associated circuitry **156**. The pads **155** and the associated circuitry **156** act as sensors and addressing circuitry and combine to form the sense electrode for a biometric input device. The analogue watch **150** is designed to be easily read in the presence of the pads **155** and the associated circuitry **156**. This is accomplished by ensuring that a short hand on the watch **150** is long enough to be partially visible at each outside edge of the metal pads **150** in each possible orientation. Alternatively, this is accomplished by designing the hands of the watch to be visible through or between the pads

150. Further alternatively, this is accomplished by designing the pads 150 such that information on positions of the watch hands is transmitted through or by the metal pads 150. Further alternatively, this is accomplished by designing the watch face with an offset analogue time indication providing sufficient space for the pads 150 as is shown in Fig. 5a.

The associated circuitry 156 is coupled to driver and sensing circuitry for reading the electrode in the form of metal pads 155 and for determining the presence of a fingerprint or other biometric input. The analogue watch 150 also comprises an infra red emitter port 55.

Alternatively in Fig. 5a and Fig. 5b, the infra red emitter port 55 comprises a transceiver capable of transmitting and receiving information in the form of infra red signals. An emitter is sufficient for carrying out the invention but a transceiver adds additional functionality. A watch, such as those shown in Figs. 5a and 5b can accept information to further enhance security of the invention during use. Further, a transceiver is useful in programming the device for password access or for new authorized users. Further, a transceiver is useful in storing a time log of accesses and providing same to a computer at intervals.

Alternatively, the emitter 55 is a wireless emitter other than infrared. Further alternatively, the emitter 55 is in the form of a coupling device for coupling to the receiving module 20 and sending a signal thereto via a non-wireless electrical connection. Alternatively, the transceiver 55 is a wireless transceiver other than infrared. Further alternatively, the transceiver 55 is in the form of a coupling device for coupling to the receiving module 20 and sending a signal thereto or receiving a signal therefrom via a non-wireless electrical connection.

Fig. 6 shows a block diagram of the transmitting module 10 of the BSIS. The module 10 comprises a power source in the form of a battery 5. The battery provides power to electronic circuits within the transmitting module 10. A reader 11 comprises a transducer, or sensor 15, 16, 17, and a drive circuit 18. The sensor is in the form of a contact imaging device for scanning a fingerprint. The contact imaging device may be in the form of Figs. 2, 3, and 4

or may be a conventional capacitive contact imaging device. Conventional capacitive contact imaging devices use a silicon substrate with an array of capacitive pads, each capacitor being associated with a driver. The sensing pads are disposed in close but non-contacting relationship. A small gap between adjacent elements ensures that adjacent edges of the elements do not wipe against one another when a finger is pressed against the sensing surface. The sensing surface is formed by film deposition on the substrate surface. Sensing pads are regularly spaced apart equally sized electrodes built by metal deposition on an appropriate glass or quartz substrate. Alternatively, the sensing pads are irregular and/or unequally spaced. A reader used for the transducer of an embodiment of the present invention is of a simplified design, adapted for large scale manufacture. The reader comprises a glass substrate 15 for supporting a capacitive array 16 and a contact surface (sheet) 17. The array 16 comprises Indium-Tungsten oxide traces which are overlapped with hard gold. Each capacitive element has a sense electrode and a switching device such that, when a finger is pressed on the contact surface 17 each sense electrode and the respective overlying portion of the finger surface form opposite plates of a capacitor, the finger surface being at ground potential. The insulating film and air gap, when present, provides the capacitor dielectric. The capacitances of these individual capacitors vary as a function of the spacing between the finger and the contact surface, with smaller capacitance values occurring where the troughs in the finger surface are aligned with a sensor than where ridges are so aligned.

Drive circuit 19 is, preferably, not disposed on the substrate as in conventional sensors. It is preferably coupled to switching devices for controlling and addressing each capacitive pad according to a mapping sequence whereby a predetermined potential is applied to each capacitive pad. When a finger is placed on sheet 17 charges are induced in array 16. Charge is induced in each capacitor in an uneven manner in dependence upon ridges and troughs in the fingertip. The sensor reads these induced charges in the form of changes in capacitance or capacitive charge and transforms them into a bitmap particular to the fingerprint or a group of fingerprints.

Alternatively, the array of capacitive plates 17 is applied to a plastic film using metal-film processing or photographic image processing techniques. The plastic film is then applied

to any surface, such as a wallet, a key chain, a pen knife, a personal digital assistant, a transportable computer or a watch. Drive circuit **19** is then attached to the array of capacitive pads using conductive epoxy adhesives, or an anisotropic adhesive process. This allows for an inexpensive sensor substrate which can be produced on a large scale using conventional LCD techniques.

The bitmap collected from the capacitive array is then input to processing unit **12** which encodes the bitmap containing the fingerprint information and generates a biometric ID. In one embodiment, processor **12** is an 8-bit microprocessor, such as Intel 8051. Processor **12** may include a standard encryption module which applies an encryption algorithm for generating an encoded biometric ID.

An infrared transmitter **19** receives the biometric ID, modulates an infrared carrier with this information and then transmits an authorization request signal to receiving module **20**.

A keypad **13** and a display **14** are preferably provided at the transmitting module **10**. Keypad **13** is used for providing further data or functionality in the form of ON/OFF functionality and a password. In the embodiment comprising a watch, display means **14** includes time information.

Receiving module **20** is shown in Fig. 7. Receiving module **20** is provided with appropriate transducer means **21** for receiving the authorization request signal and converting it into an electrical signal. Transducer **21** may be for example an IrDA diode. The transducer is controlled by a control Unit **25** in dependence upon the current operating mode as determined by a mode selector **26**. Modes of operation for the device are discussed below. The converted electrical signal is applied to decoder **22** where the biometric ID is extracted in the conventional mode. The recovered biometric IDC and a reference IDREF are applied to a comparator **23**. The reference ID is obtained from a memory **24**, where it has been previously stored, using any of the conventional methods. If a password is also included in the received signal together with the biometric IDC, the password is extracted by decoder **22** in addition to the biometric IDC, and compared with a reference password in comparator **23**. When the

result of the comparison indicates that the biometric IDC and the password are acceptable, access to the host system is permitted.

The receiving module **20** is initially configured in an ENROLL mode for obtaining and for storing one or more reference biometric samples. Enrolling software is normally inaccessible after the first use, or in a multi-user system, re-entering the enroll mode is accomplished through a function key and is limited to an authorized person or authorized persons. After enrollment is completed, the module enters its NORMAL mode.

The flow chart of Fig. 8 shows the operation of an embodiment of the invention. In step **30**, the biometric data is read at the transmission module **10** with reader **11**. As indicated above, in a preferred embodiment, reader **11** collects data indicative of the image of a fingerprint. Next, the biometric data is encoded in processing means **12**, in step **31**. Transmitter **16** broadcasts the biometric data, as illustrated in step 32. Next, in step **33**, receiving module **20** receives the biometric data and decodes the biometric ID therefrom, and checks the mode indicator in step **34**. When the receiving module is in the "enroll" mode, the biometric ID is stored in memory **24** in step **35**, and the receiving module is switched to the "access" mode of operation in step **36**.

When the receiving module **20** is in the "access" mode, the received biometric ID is compared with the reference biometric ID in step **37**. If the received signal comprises also a password, receiving module **20** separates the password from the biometric ID, and additionally compares the password against a reference password in step **38**. Finally, access to the host system is authorized or not, depending on the result of the comparison(s), as shown in steps **39** and **40** respectively.

Alternatively, the transmitting module **10** is provided with a a change password initiator in the form of a key or a button allowing a user of the transmitting module **10** to enter a mode to alter their password. In this embodiment, an initial arbitrary password (such as none or "password") is set. Entering the mode to alter the password requires user verification of the existing password, user entry of a new password and user verification of

the new password. Password selection algorithms of this type are known in the art of computer network security and operating systems. The password is stored in the receiving module 20. Alternatively, the password is stored in the transmitting module **10**.

Referring to Fig. 9 a flow chart of an embodiment wherein biometric data authentication is performed within the transmitting module **10** and an access key is transmitted therefrom to the receiving module **20** is shown. Only "access" mode is described for this embodiment, "enroll" mode functions in a fashion similar to that set out above. This embodiment is particularly useful in that theft of the transmitting module **10** is discouraged.

The biometric data is read at the transmission module **10** with reader **11**. As indicated above, in a preferred embodiment, reader **11** collects data indicative of the image of a fingerprint. Next, the biometric data is decoded for comparison. The decoding accounts for rotation and misalignment in the biometric input. The decoded data is compared to at least previously stored biometric data. When password protection is also used, a password is required and verified. When the verification of the password and the fingerprint fails (i.e. the password is incorrect or the decoded biometric data failed to register correctly against any previously stored biometric data) no further action occurs. Alternatively, a signal indicative of invalid registration is transmitted. Further alternatively, the signal contains information in the form of the biometric data to identify the unauthorized user of the device. When the verification succeeds the biometric data is encoded in processing means **12**. Alternatively, an access key is encoded in processing means **12**.

Transmitter **16** broadcasts the encoded data to the receiving module **20** which receives the encoded data and decodes it. At the receiving module (not shown), the data is verified to be an acceptable user authorization and provides access to the host system or releases a host locking mechanism.

Referring to Fig. **10** a flow chart of an embodiment of the present invention using bi-directional communication is shown. Biometric information is read from a biometric input means. The information is decoded and then stored in an electronic storage means. The

electronic storage means is in the form of RAM. Alternatively, the electronic storage means comprises magnetic storage means, optical storage means, mechanical storage means, or other suitable low power storage means. The decoded information is analyzed to determine whether the information corresponds to an authorized user of the host system. When an authorized user is detected through a comparison, an access code is stored in a buffer. When the biometric information does not correspond to an authorized user, an error code is stored in the buffer. In response to a request from an external system for the code stored within the buffer, either the error code or the authorization code (whichever was last stored) is provided. The external system responds to the code in a predetermined fashion.

Referring to Fig. 11, a flow chart for an embodiment similar to that of Fig. 10 is shown. The flow chart of Fig. 11 shows only the lower portion of the flow chart - those parts associated with bi-directional communication. A time-out is introduced upon storage of a code. When a request is not presented within a predetermined time, the buffer is erased and the method returns to a start. This prevents use of a device, embodying a method according to this invention, when found or taken by clearing any data related to the biometric input from the buffer. Second, a request from an external system comprises a further code parameter. The code parameter may be in the form of an encryption key, an access category, a device number, etc. According to the flow chart, a default code is provided to the external system when the received code parameter is unknown. When the code parameter is known, an access code in dependence upon the code parameter is provided to the external system. The method then returns to a start.

Referring to Fig. 12, a credit card biometric input device is shown. The device comprises a substantially flat substrate **209**. A biometric input means **210** in the form of a finger print detector is disposed on the substrate as is a battery **211**, an edge connector **212**, actuating means **214** in the form of card edges, and electronic circuitry **215**. The circuitry comprises electronic storage and processing means for verifying biometric input and providing an access code. The processor means is also for accepting a parameter code from an external system and encrypting the access code before transmitting same. In use, a user of such a device places their finger tip onto the biometric input means **210**. Their fingerprint is

recorded, analyzed, and verified in the electronic storage and processor means **215**. When the user is authorized, an access code is stored in a buffer and a time-out is put in place. When a request for the access code is provided prior to the time-out, the access code is transmitted. The device may also function according to the flow charts of Figs. 8, 9, 10, and 11.

The embodiment of Fig. 12, is useful as a credit card and for electronic finance. Unattended electronic devices accept the card in a similar fashion to current automatic teller machines (ATM) and only return the card when it is not reported stolen. Attended transaction locations, such as stores, would erase the buffer and require input of the biometric information in their presence. In this way, the device serves the purpose of both a credit card and an electronic "cash" card.

In Fig. 13 a key chain embodiment of the invention is shown. The key chain **220** is attached to a biometric input device **209a** comprising biometric input means 210, buttons 218, an infrared transceiver **219a**, and electronic circuitry (not shown) housed within the device. In operation the device acts like other devices described above. The buttons may be used for password entry, function selection, or to distinguish operations such as opening a car door, a garage door, a trunk for a car, etc.

In Fig. 14 a further key chain embodiment of the invention is shown. The key chain **220** is attached to a biometric input device **209a** comprising biometric input means **210**, buttons **218**, an RF transceiver **219b**, and electronic circuitry (not shown) housed within the device. In operation the device acts like other devices described above. The buttons may be used for password entry, function selection, or to distinguish operations such as opening a car door, a garage door, a trunk for a car, etc. In an embodiment, uni-directional communication is used between a portable biometric input device according to this invention and a receiving module. Alternatively, biometric data authentication is performed using two way communications between the transmitting module **10** and the receiving module **20**. Further alternatively, biometric data authentication is performed using multi-channel multi-party communications to add functionality such as access logs, central access control, access permission authorization from a third location, etc.

In a further embodiment, the transmitting module **10** and the receiving module **20** are programmed via a communication port using a computer. The communication port is preferably bi-directional. Preferably, the communication port is the transceiver in the transmitting module **10** and the transducer in the receiving module **20**.

A device according to the present invention may be used to provide secure access to computers. computer networks, buildings, safes, houses, portable electronic locks, automobiles, banking services in the form of automatic teller machines, electronic commerce, household cabinets for rendering them child safe, television services, pay per view television services. electrical appliance, garages, hotel rooms, educational facilities. health club facilities, etc. The device is useful where passwords, magnetic strips, physical key and lock mechanisms, electronic locks, ID cards and other secure forms of identification are used.

In a further embodiment and according to a method according to the present invention, the transmitter is an audio transmitter capable of transmitting tones in dependence upon the biometric data. One form of the tones is a series of telephone tones indicative of the identity of an individual and capable of being understood by a telephone system. A further form of tones are similar to those of a computer modem or fax machine. devices sending digital data across analogue telephone lines.

In order to improve the security of embodiments of this invention. it is possible to employ encryption technology. The encryption technologies are generally known and include public/private key encryption, session key encryption, and other encryption schemes for secure data transmission. In private/public key encryption, a receiver sends a public key to a device according to the present invention and transmissions from the device to the receiver are encrypted using the public key. Only the receiver, having the private key, can decrypt the transmission. A group of public keys can be used or public keys can vary regularly in order to prevent interception and replay of a transmission.

In session key encryption an encryption key is selected for a particular session based on a predetermined algorithm or some other method. The key is used for the session and then

discarded. In this fashion, interception and recording of transmitted signals is of no use as the session key will change for subsequent sessions.

It is also suggested to increase security by verifying the device type in use according to the invention. Establishing a device type and protocol allows some receivers to inhibit access to devices of certain security access levels or protocols.

Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What we claim is:

1. A portable biometric input device comprising:
biometric sensing means for sensing biometric input information, generating biometric data therefrom, and providing the biometric data in relation to the sensed biometric input information;
transmission means for receiving at least an aspect of the biometric data and for transmitting a signal in dependence upon the at least an aspect of the biometric data; and
a battery for providing power to the device.

2. A portable biometric input device as defined in claim 1 wherein the transmission means is a wireless transmission means for transmitting a signal in dependence upon the at least an aspect of the biometric data.

3. A portable biometric input device as defined in claim 1 wherein the transmission means comprises a biometric data encoder and an infrared transmitter for transmitting a signal in dependence upon the at least an aspect of the biometric data.

4. A portable biometric input device as defined in claim 1 further comprising storage means for storing data related to said biometric data.

5. A portable biometric input device as defined in claim 4 further comprising processor means for processing the biometric data.

6. A portable biometric input device as defined in claim 5 wherein the processor means is for comparing the biometric data with previously stored biometric data to provide comparison results; and the signal in dependence upon at least an aspect of the biometric data comprises a signal in dependence upon the comparison results.

7. A portable biometric input device as defined in claim 1, further comprising means to receive a password and wherein the transmission means is for transmitting a signal in dependence upon at least an aspect of the biometric data and the password.

8. A portable biometric input device as defined in claim 1, further comprising means to receive a password and wherein the processor means is for comparing the biometric data with previously stored biometric data and the password and a previously stored password to provide comparison results; and the signal in dependence upon at least an aspect of the biometric data comprises a signal in dependence upon the comparison results.

9. A portable biometric input device as defined in claim 1, further comprising means for encrypting at least an aspect the biometric data; and the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data.

10. A portable biometric input device as defined in claim 9 wherein the means for encrypting the biometric data comprise public/private key encryption means.

11. A portable biometric input device as defined in claim 9 wherein the means for encrypting the biometric data comprise session key encryption means.

12. A portable biometric input device as defined in claim 1 wherein the biometric input means is a fingerprint imaging device.

13. A portable biometric input device as defined in claim 1 further comprising a housing in the form of a watch casement and a watch face.

14. A portable biometric input device as defined in claim 13 wherein the biometric input means comprises associated electronic circuitry and conductive pads disposed on the watch face.

15. A portable biometric input sensor comprising:

a) an array of sense elements spaced apart and comprising a sensing electrode for sensing biometric input;

b) drive means coupled to at least some of the sense elements for controlling and addressing each of the at least some sense elements according to a predetermined sequence, for receiving a signal in dependence upon the biometric input, and for providing biometric data in dependence upon the sensed biometric input;

(c) processor means for processing biometric data; and,

(d) wireless transmission means for transmitting to a receiver a signal that corresponds to at least an aspect of the biometric data.

16. A portable biometric input sensor as defined in claim 15, further comprising means for encrypting the biometric data further comprising means for encrypting at least an aspect the biometric data; and the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data.

17. A portable biometric input sensor as defined in claim 16 wherein the means for encrypting the biometric data comprise public/private key encryption means.

18. A portable biometric input sensor as defined in claim 16 wherein the means for encrypting the biometric data comprise session key encryption means.

19. A biometric security identification system comprising:

a portable transmitting module comprising a biometric sensing means, means for encoding biometric data and wireless transmission means for transmitting the encoded biometric data as an encoded signal; and

a receiving module comprising means for receiving the encoded signal, means for extracting the encoded biometric data, and means for comparing the encoded biometric data with predetermined reference values, and means for authorizing access to a host system.

20. A biometric security identification system as defined in claim 19, wherein said biometric sensing means comprises a fingerprint scanner.

21. A biometric security identification system as defined in claim 19, further comprising means for encrypting the biometric data further comprising means for encrypting at least an aspect the biometric data; the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data; and the means for extracting the encoded biometric data comprises means for decrypting and for extracting the encoded biometric data.

22. A biometric security identification system as defined in claim 21 wherein the means for encrypting the biometric data comprise public/private key encryption means.

23. A biometric security identification system as defined in claim 21 wherein the means for encrypting the biometric data comprise session key encryption means.

24. A portable biometric input device comprising:
sensing means including a platen upon which to rest a finger, said sensing means for sensing the presence and location of fingerprint ridges upon the device;
processor means for processing sensed data; and,
wireless transmission means for transmitting a signal that corresponds to at least an aspect of the sensed data; and
a battery for providing power to the device.

AMENDED CLAIMS

[received by the International Bureau on 4 February 1998 (04.02.98); original claims 1-24 replaced by new claims 1-18 (4 pages)]

1. A portable biometric input device comprising:

biometric sensing means for sensing biometric input information, generating biometric data therefrom, and providing the biometric data in relation to the sensed biometric input information;

storage means for storing data related to said biometric data;

processor means for characterising the biometric data; and,

transmission means for receiving at least an aspect of the characterised biometric data and for transmitting a signal in dependence upon the at least an aspect of the characterised biometric data; and

a battery for providing power to the device.

2. A portable biometric input device comprising:

biometric sensing means for sensing biometric input information, generating biometric data therefrom, and providing the biometric data in relation to the sensed biometric input information;

a processor for comparing the biometric data with previously stored biometric data to provide comparison results; and,

transmission means for receiving at least an aspect of the biometric data and for transmitting a signal in dependence upon the comparison results.

3. A portable biometric input device as defined in claim 2, further comprising means to receive a password and wherein the transmission means is for transmitting a signal in dependence upon at least an aspect of the biometric data and the password.

4. A portable biometric input device as defined in claim 2 comprising means to receive a password and wherein the processor means is for comparing the password and a previously stored password to provide further comparison results; and wherein the signal in dependence upon at least an aspect of the comparison results is a signal

in dependence upon at least an aspect of the comparison results and of the further comparison results.

5. A portable biometric input device comprising:

biometric sensing means for sensing biometric input information, generating biometric data therefrom, and providing the biometric data in relation to the sensed biometric input information;

means for encrypting at least an aspect the biometric data;

transmission means for receiving at least an aspect of the encrypted biometric data and for transmitting a signal in dependence upon the at least an aspect of the biometric data; and

a battery for providing power to the device.

6. A portable biometric input device as defined in claim 5 wherein the means for encrypting the biometric data comprise public/private key encryption means.

7. A portable biometric input device as defined in claim 5 wherein the means for encrypting the biometric data comprise session key encryption means.

8. A portable biometric input device as defined in claim 1 wherein the biometric input means is a fingerprint imaging device.

9. A portable biometric input device as defined in claim 1 further comprising a housing in the form of a watch casement and a watch face.

10. A portable biometric input device as defined in claim 9 wherein the biometric input means comprises associated electronic circuitry and conductive pads disposed on the watch face.

11. A portable biometric input sensor comprising:

a) an array of sense elements spaced apart and comprising a sensing electrode for sensing biometric input;

b) drive means coupled to at least some of the sense elements for controlling and addressing each of the at least some sense elements according to a predetermined sequence, for receiving a signal in dependence upon the biometric input, and for providing biometric data in dependence upon the sensed biometric input;

(c) processor means for processing biometric data; and,

(d) wireless transmission means for transmitting to a receiver a signal that corresponds to at least an aspect of the biometric data.

12. A portable biometric input sensor as defined in claim 11, further comprising means for encrypting the biometric data further comprising means for encrypting at least an aspect the biometric data; and the transmission means is for receiving the encrypted data and for transmitting a signal in dependence upon the at least an aspect of the encrypted data.

13. A portable biometric input sensor as defined in claim 12 wherein the means for encrypting the biometric data comprise public/private key encryption means.

14. A portable biometric input sensor as defined in claim 12 wherein the means for encrypting the biometric data comprise session key encryption means.

15. A biometric security identification system comprising:

a portable transmitting module comprising a biometric sensing, means for sensing biometric data, means for encrypting at least an aspect the biometric data, means for encoding the encrypted biometric data, and wireless transmission means for transmitting the encoded encrypted biometric data as an encoded signal; and

a receiving module comprising means for receiving the encoded signal, means for extracting the encoded biometric data, means for decrypting the decoded biometric data, means for comparing the biometric data with predetermined reference values, and means for authorizing access to a host system.

16. A biometric security identification system as defined in claim 15, wherein said biometric sensing means comprises a fingerprint scanner.

17. A biometric security identification system as defined in claim 15 wherein the means for encrypting the biometric data comprise public/private key encryption means.

18. A biometric security identification system as defined in claim 15 wherein the means for encrypting the biometric data comprise session key encryption means.

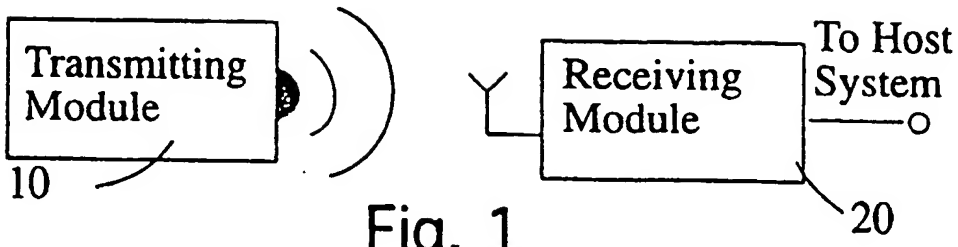


Fig. 1

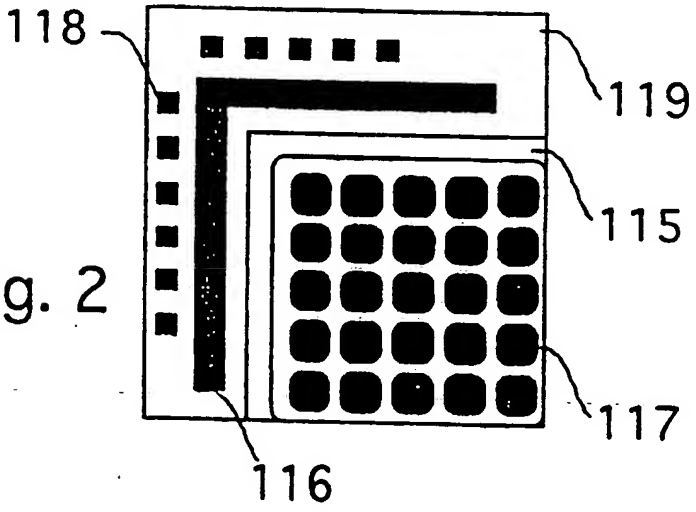


Fig. 2

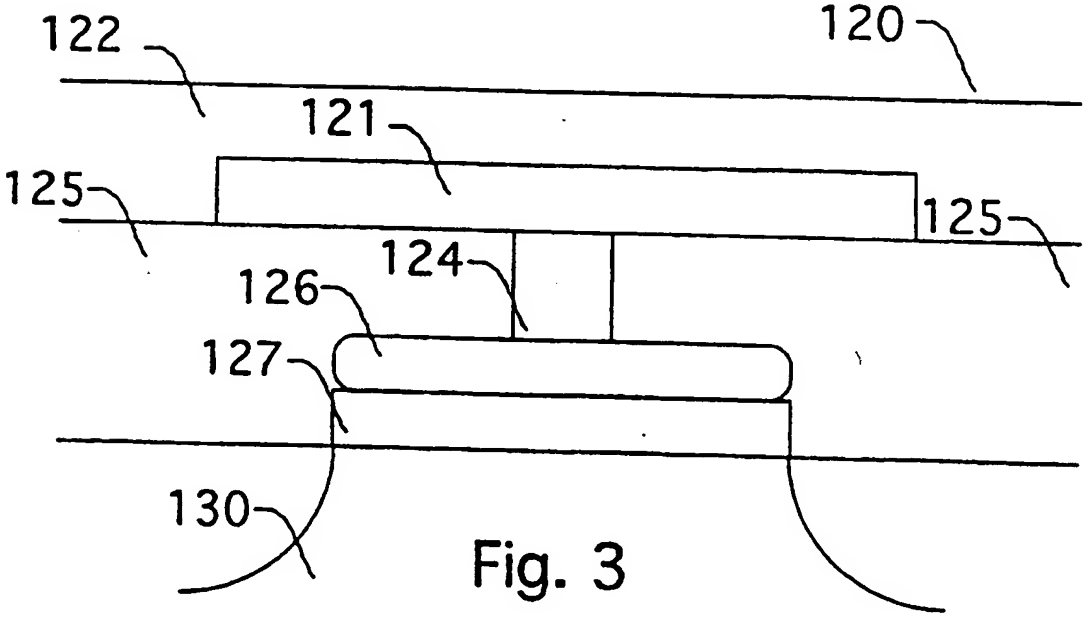


Fig. 3

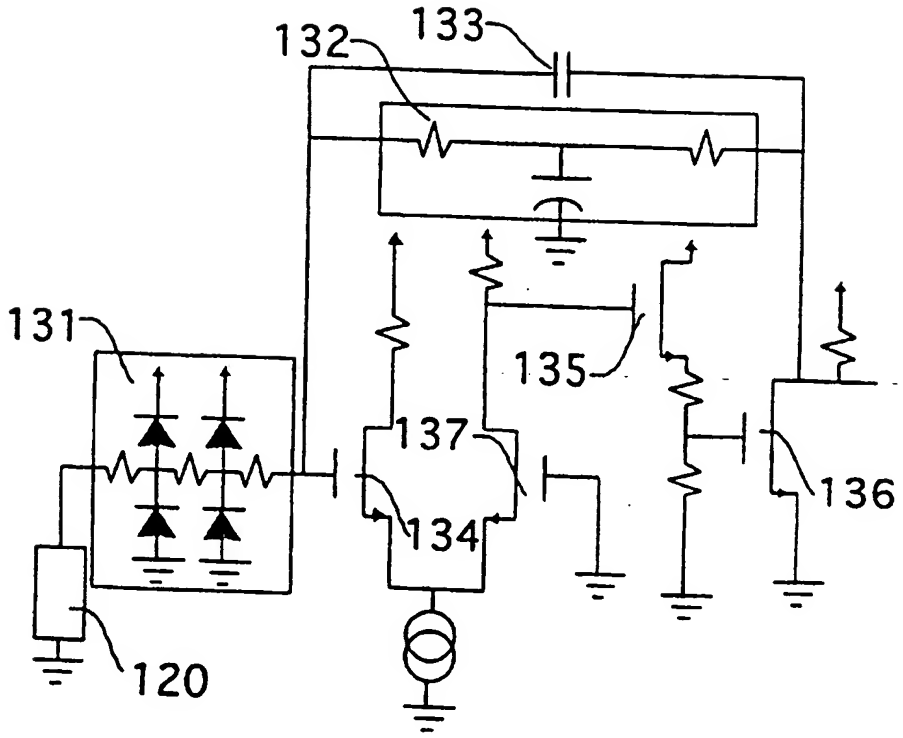


Fig. 4

Fig. 5a

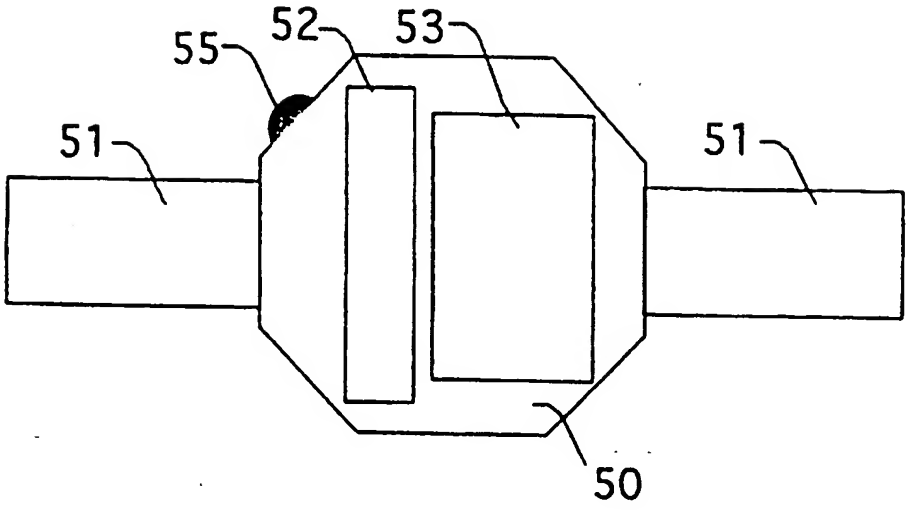
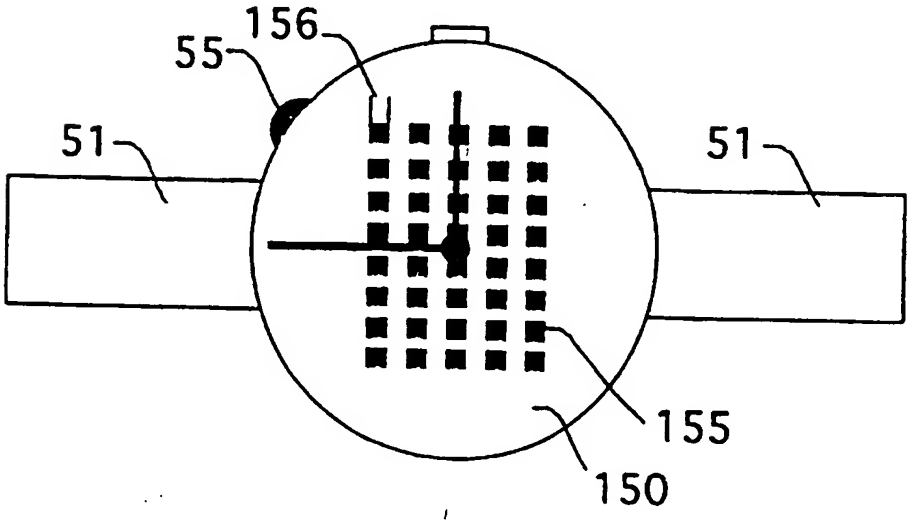


Fig. 5b



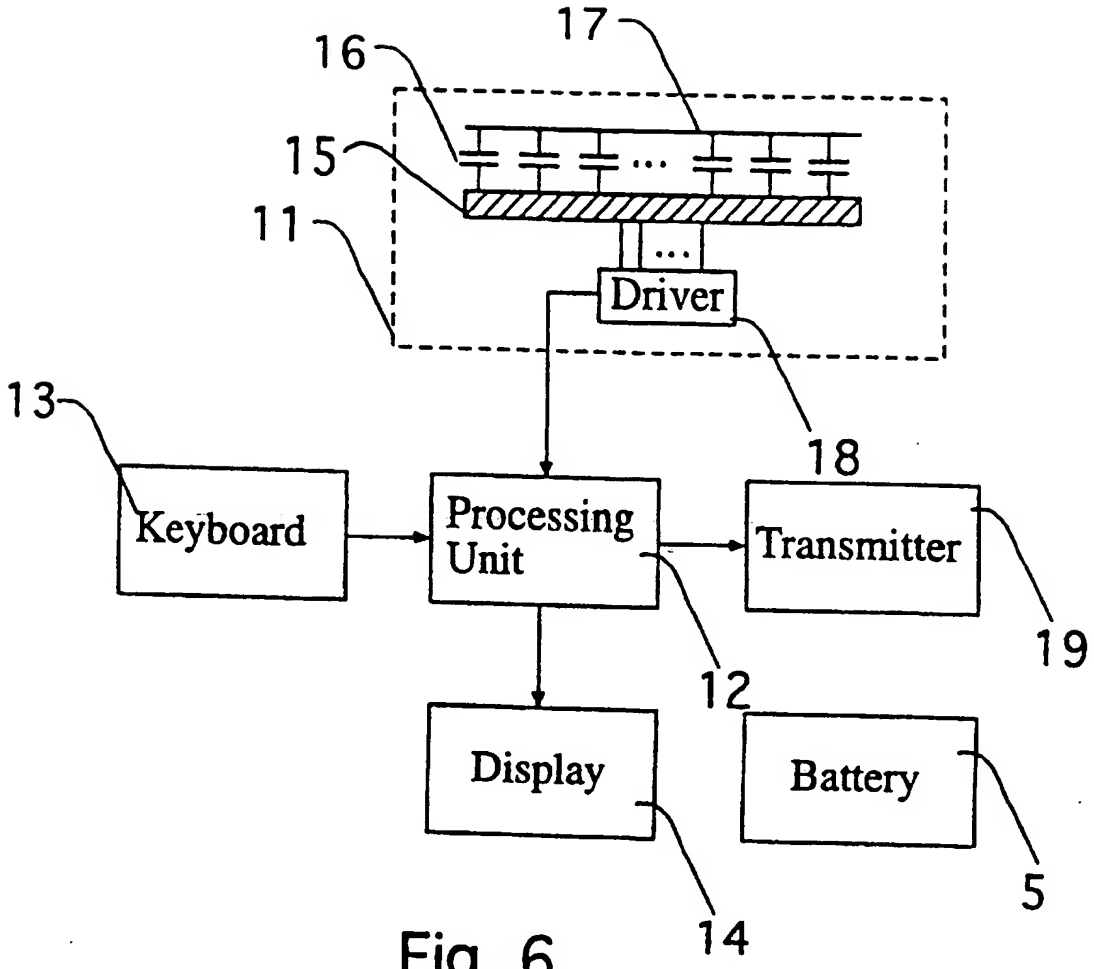

17
16
15
11
Driver
13
18
Keyboard
Processing Unit
Transmitter
19
12
Display
Battery
5
14

Fig. 6

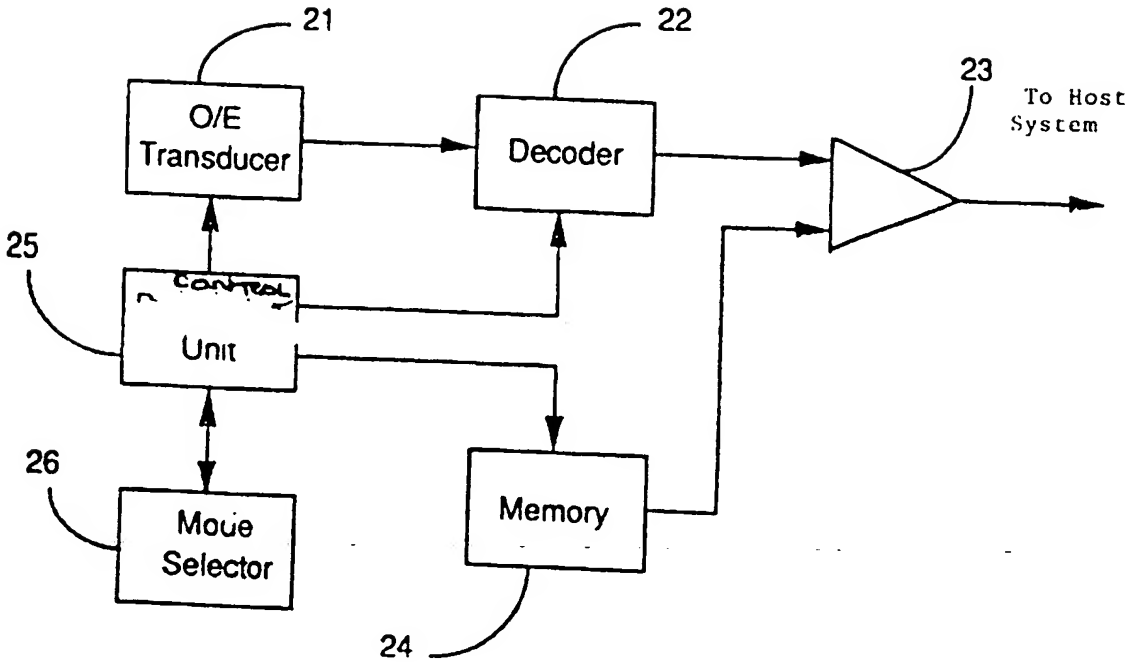

21
22
23
To Host System
O/E Transducer
Decoder
25
Control Unit
26
Mode Selector
Memory
24

FIGURE 7

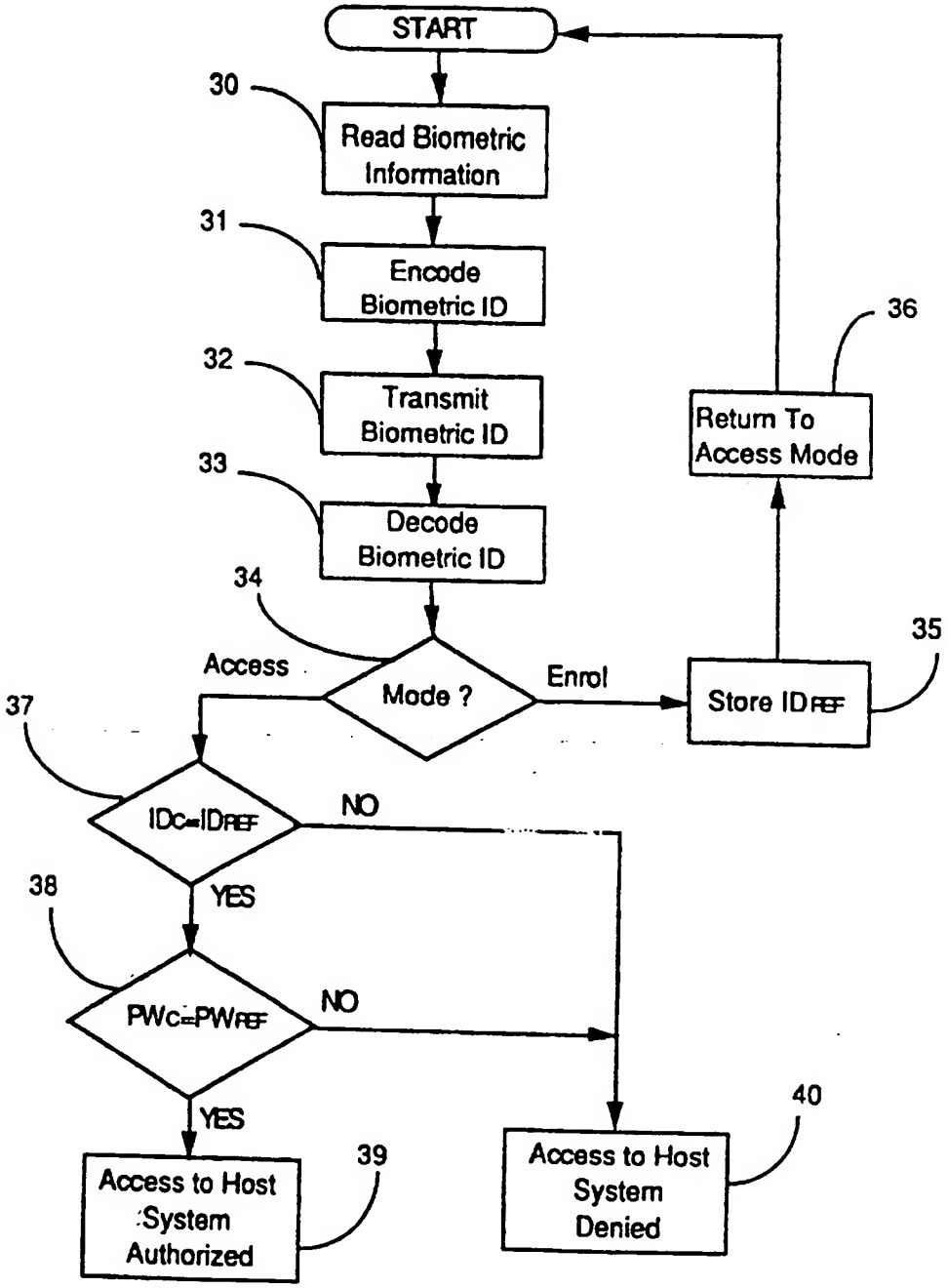

START
30
Read Biometric Information
31
Encode Biometric ID
32
Transmit Biometric ID
33
Decode Biometric ID
34
Access
Mode ?
Enrol
35
Store ID REF
36
Return To Access Mode
37
IDc=IDREF
NO
YES
38
PWc=PWREF
NO
YES
39
Access to Host System Authorized
40
Access to Host System Denied

FIGURE 8

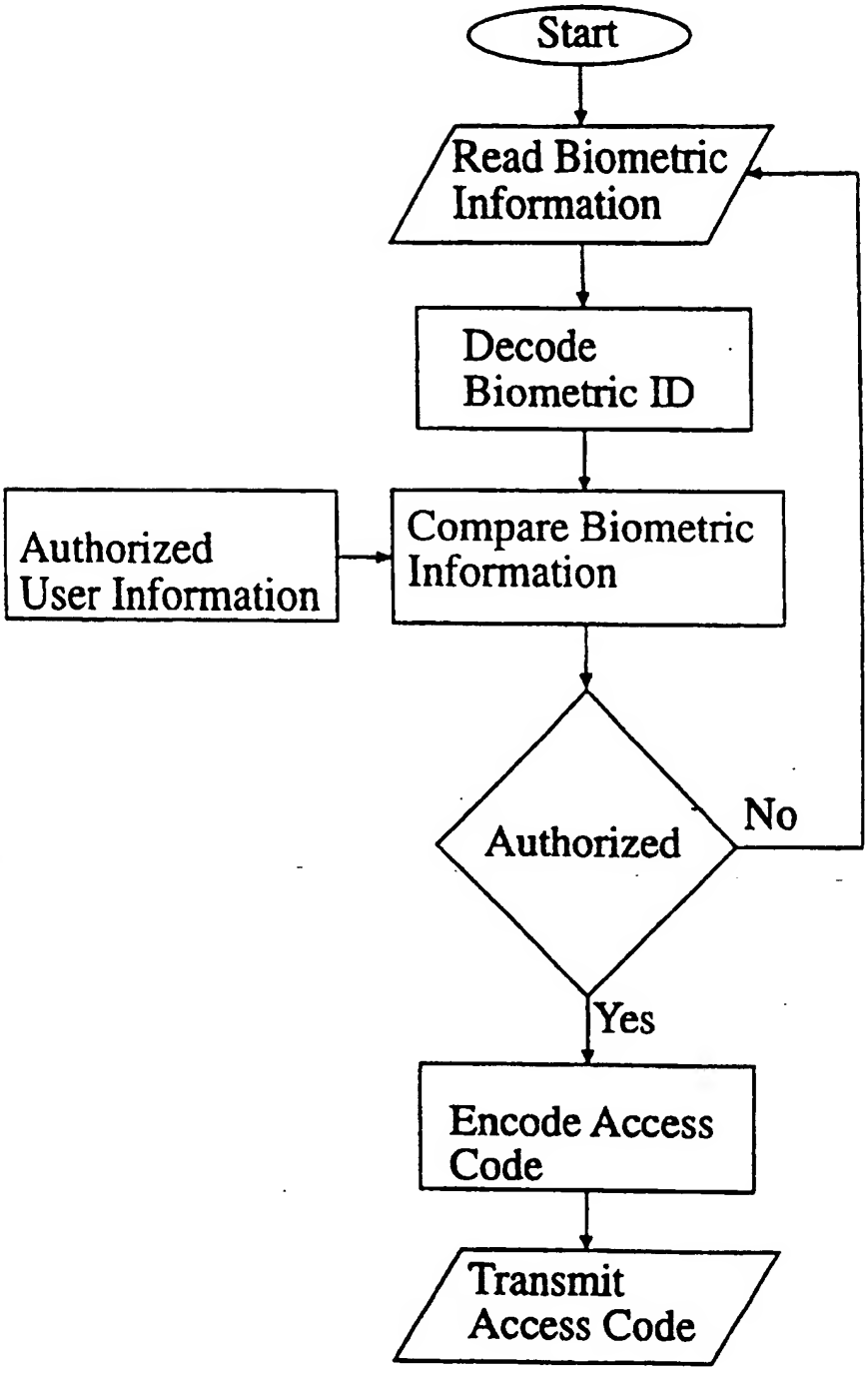

Start
Read Biometric Information
Decode Biometric ID
Authorized User Information
Compare Biometric Information
Authorized
No
Yes
Encode Access Code
Transmit Access Code

Fig. 9

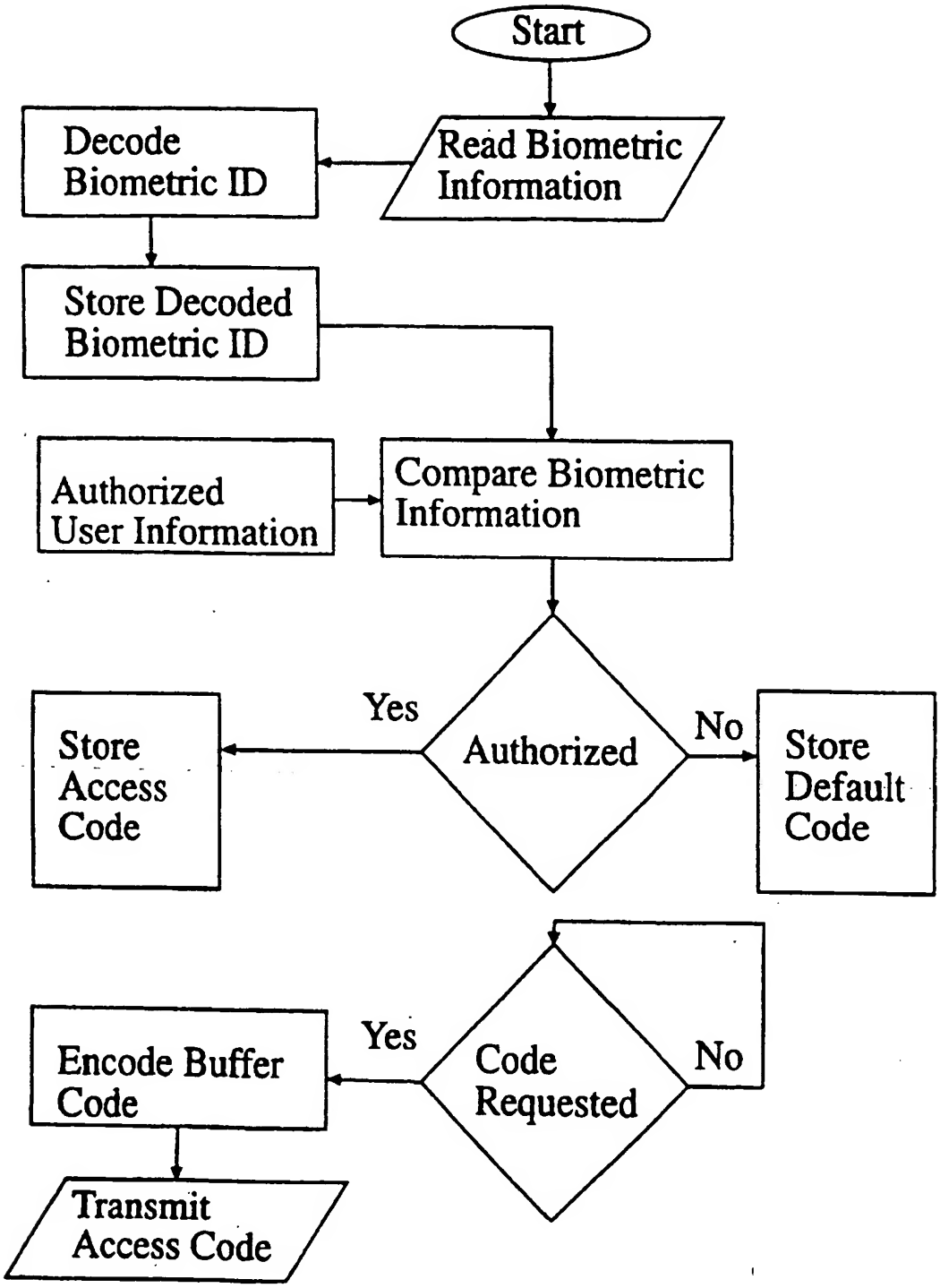

Start
Read Biometric Information
Decode Biometric ID
Store Decoded Biometric ID
Authorized User Information
Compare Biometric Information
Authorized
Yes
No
Store Access Code
Store Default Code
Code Requested
Yes
No
Encode Buffer Code
Transmit Access Code

Fig. 10

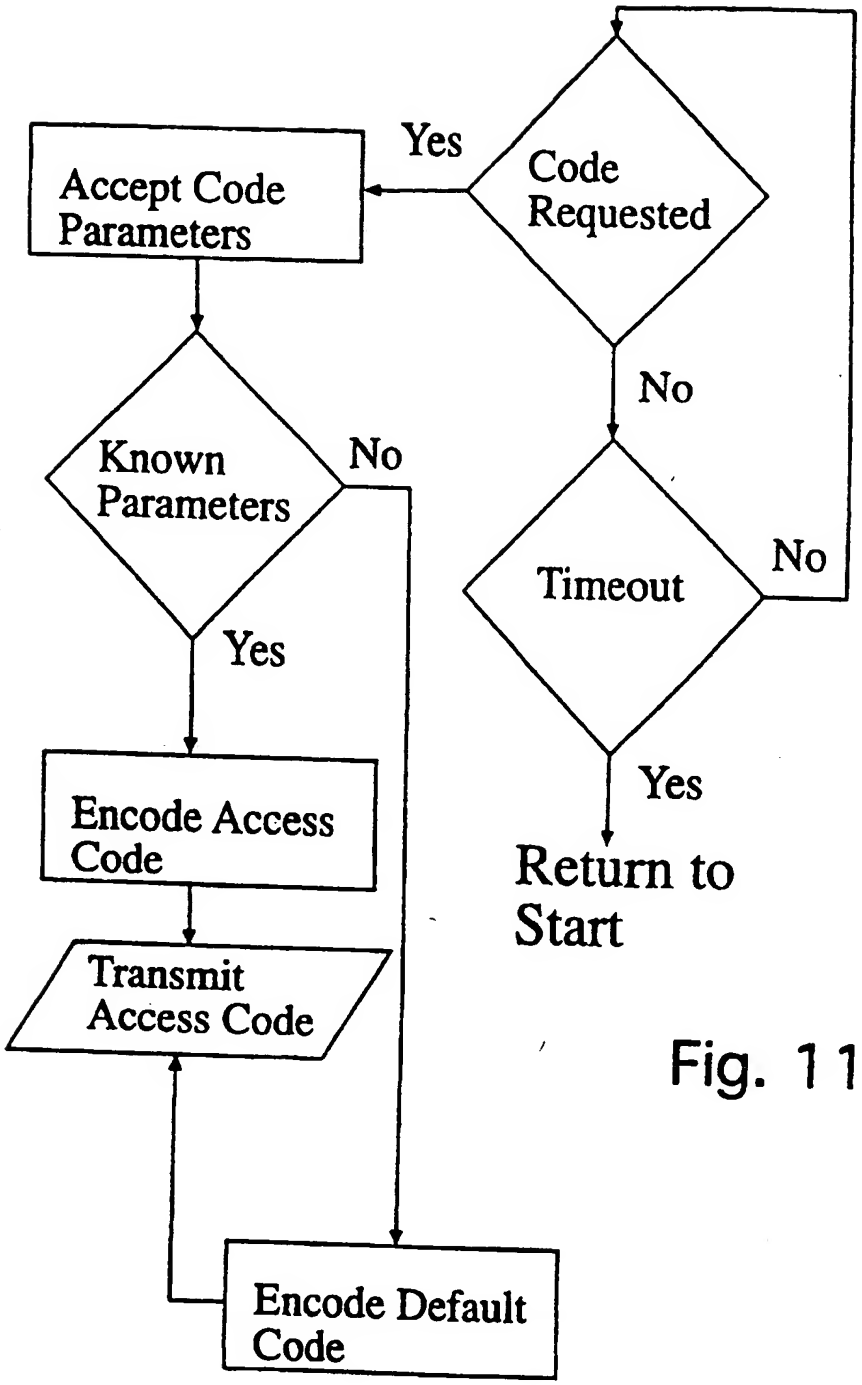

Code Requested
Yes
Accept Code Parameters
No
Known Parameters
No
Timeout
No
Yes
Yes
Encode Access Code
Return to Start
Transmit Access Code
Encode Default Code

Fig. 11

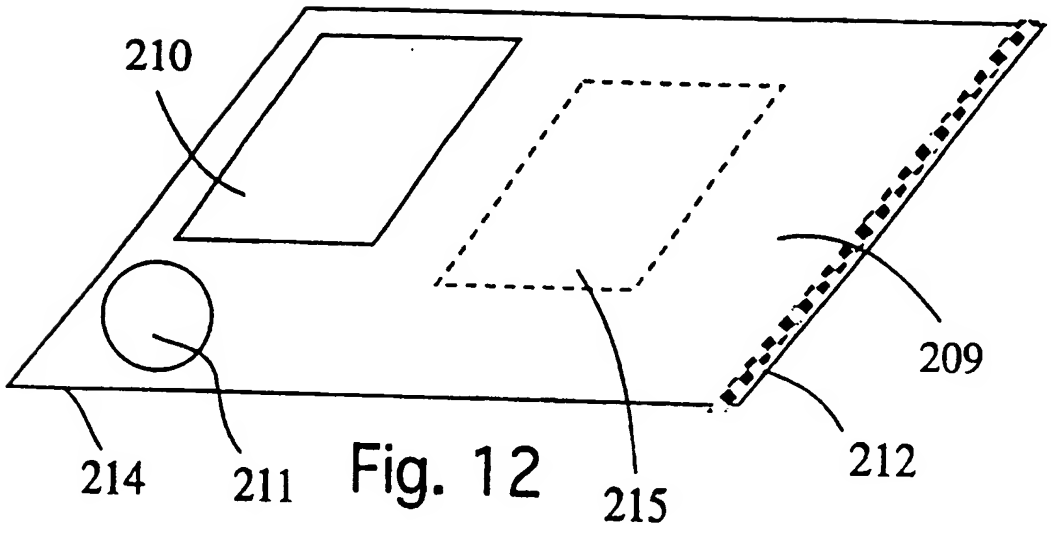


Fig. 12

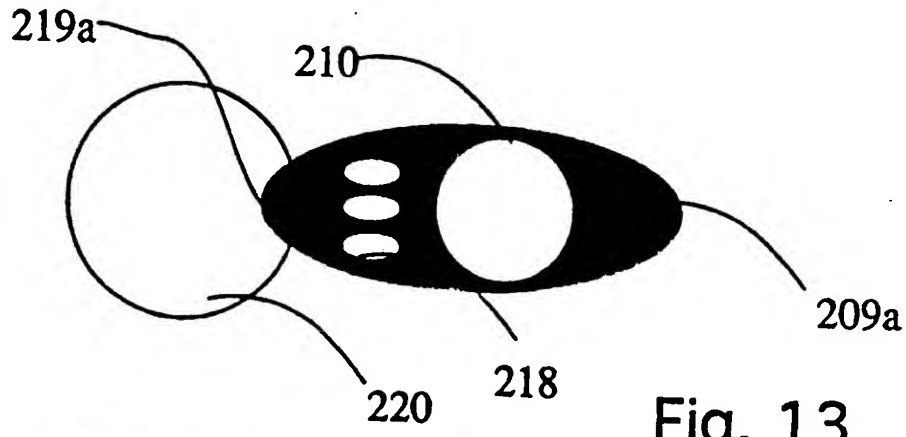


Fig. 13

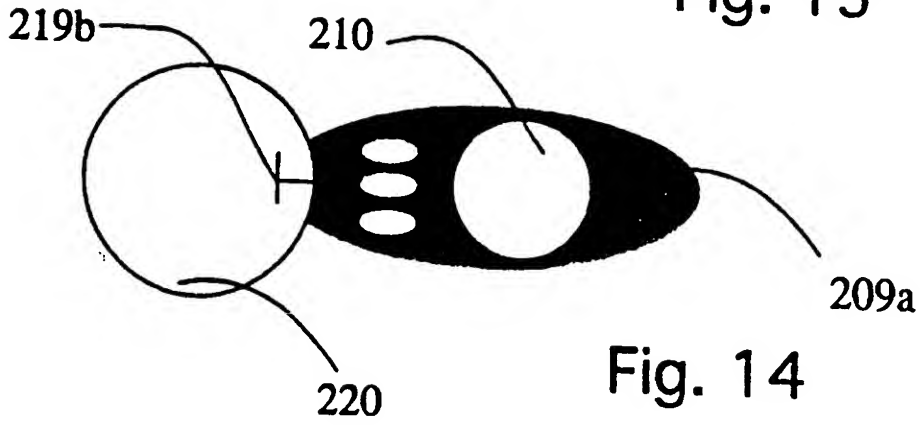


Fig. 14

INTERNATIONAL SEARCH REPORT

Interr. al Application No
PCT/CA 97/00663

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00 G06F1/00

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 181 582 A (BLACKWELL VICTOR CAMPBELL) 23 April 1987 see abstract; figures 1-6 see page 1, line 66 - page 4, line 10	1-6, 12-14, 19,20,24
Y		7-10,15, 21,22

Y	US 4 993 068 A (PIOSENKA GERALD V ET AL) 12 February 1991 see abstract; figures 1-3 see column 2, line 61 - column 3, line 8 see column 4, line 61 - column 5, line 19 see column 5, line 52 - line 64 see column 9, line 22 - line 31	7-10,21, 22
A		16,17

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 1997	04/12/1997

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interi ıal Application No
PCT/CA 97/00663

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category '	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 577 345 A (ABRAMOV IGOR) 18 March 1986 see the whole document	15
A	EP 0 661 675 A (IBM) 5 July 1995 see column 3, line 35 - column 4, line 25 see claims 16,17	11,18,23

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 97/00663

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2181582 A	23-04-87	AU 6476786 A	05-05-87
		EP 0241504 A	21-10-87
		WO 8702491 A	23-04-87
US 4993068 A	12-02-91	NONE	
US 4577345 A	18-03-86	NONE	
EP 0661675 A	05-07-95	US 5526428 A	11-06-96
		BR 9405190 A	08-08-95
		CN 1123434 A	29-05-96
		JP 7210643 A	11-08-95